DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

Docket No. USCBP-2020-0051

RIN 1651-AB30

Privacy Act of 1974: Implementation of Exemptions; U.S. Department of Homeland Security/U.S. Customs and Border Protection-018 Customs Trade Partnership Against Terrorism System of Records.

AGENCY: U.S. Customs and Border Protection, U.S. Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The U.S. Department of Homeland Security (DHS) is giving concurrent notice of a modified and reissued system of records pursuant to the Privacy Act of 1974 for the "DHS/U.S. Customs and Border Protection (CBP)-018 Customs Trade Partnership Against Terrorism System of Records," and this proposed rulemaking. In this proposed rulemaking, the Department and CBP proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number USCBP-2020-0051, by one of the following methods:

- Federal e-Rulemaking Portal**:** http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax**:** 202-343-4010.

- Mail**:** James Holzer, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Debra Danisek, Privacy.CBP@cbp.dhs.gov, (202) 344-1610, CBP Privacy Officer, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229. For privacy issues, please contact: James Holzer, Privacy@hq.dhs.gov, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) proposes to modify and reissue a current DHS system of records titled, "DHS/CBP-018 Customs Trade Partnership Against Terrorism System of Records." DHS/CBP is reissuing this modified system of records notice to update its description of how CBP collects and maintains information pertaining to prospective, ineligible, current, or former trade partners in the CTPAT Program; other entities and individuals in their supply chains; and members of foreign governments' secure supply chain programs that have been recognized by CBP, through a mutual recognition arrangement or comparable arrangement, as being compatible with CTPAT. DHS/CBP is updating this system of records notice to clarify that CTPAT Program members may also submit information to

DHS/CBP under the CTPAT Trade Compliance program, to include importer self-assessments and other documentation.

CBP uses the information collected and maintained through the CTPAT security and trade compliance programs to carry out its trade facilitation, law enforcement, and national security missions. In direct response to 9/11, CBP challenged the trade community to partner with the government to design a new approach to supply chain security—one that protects the United States from acts of terrorism by improving security while facilitating the flow of compliant cargo and conveyances. The result was the CTPAT Program—a voluntary government/private sector partnership program in which certain types of businesses agree to cooperate with CBP in the analysis, measurement, monitoring, reporting, and enhancement of their supply chains.

Businesses accepted into the CTPAT Program are called partners and agree to take actions to protect their supply chain, identify security gaps, and implement specific security measures and best practices in return for facilitated processing of their shipments by CBP. The CTPAT Program focuses on improving security from the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination. The current security guidelines for CTPAT Program members address a broad range of topics including personnel, physical, and procedural security; access controls; education, training, and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. These guidelines offer a customized solution for the members, while providing a clear minimum standard that approved companies must meet.

Businesses eligible to fully participate in the CTPAT Program include U.S. importers; exporters; U.S./Canada highway carriers; U.S./Mexico highway carriers; rail and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/terminal operators; U.S. freight consolidators; ocean transportation intermediaries and non-

operating common carriers; Mexican and Canadian manufacturers; and Mexican long-haul carriers.

CTPAT Program members in good standing may optionally participate in the CTPAT Trade Compliance program. Beginning in March 2020, the former Importer-Self Assessment (ISA) Program was integrated into the CTPAT Program as CTPAT Trade Compliance. DHS/CBP is updating this SORN to clarify the additional records collected as part of the CTPAT Trade Compliance program, which is limited to existing CTPAT Program members. To qualify for the CTPAT Trade Compliance program, an importer must submit an additional application via the CTPAT web portal and a) be a Member of the CTPAT Security Program and in good standing, b) meet the eligibility criteria laid out in the Eligibility Questions, and c) complete a Memorandum of Understanding (MOU) and Program Questionnaire.

To participate in the CTPAT Program, a company is required to submit a confidential, on-line application using the CTPAT Security Link Portal, https://ctpat.cbp.dhs.gov. The CTPAT Security Link Portal is the public-facing portion of the CTPAT system used by applicants to submit the information in their company and supply chain security profiles.

Additionally, the applicant business must complete a Supply Chain Security Profile (SCSP). The information provided in the SCSP is a narrative description of the procedures the applicant business uses to adhere to each CTPAT Security Criteria or Guideline articulated for their particular business type (e.g., importer, customs broker, freight forwarder, air, sea, and land carriers, contract logistics providers) together with any supporting documentation. Data elements entered by the applicant business are accessible for update or revision through the CTPAT Security Link Portal. An applicant's SCSP must provide supply chain security procedures for each business in the applicant's supply chain, even if those businesses are not, or do not desire to become, partners of

CTPAT separately. This information is focused on the security procedures of those businesses (e.g., whether the business conducts background investigations on employees), rather than the individuals related to those businesses (e.g., a list of employee names).

A fuller description of this modified SORN can be found herein the Federal Register.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-018 Customs-Trade Partnership Against Terrorism (CTPAT) system of records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as

otherwise permitted by the Privacy Act. The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed and provide an opportunity for public comment.

DHS is claiming exemptions from certain requirements of the Privacy Act for the DHS/CBP-018 CTPAT System of Records. Some information in the DHS/CBP-018 CTPAT System of Records relates to official DHS national security, law enforcement, and immigration activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes or to avoid disclosure of activity techniques. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A system of records notice for the DHS/CBP-018 CTPAT System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. Amend the authority citation for Part 5 to read as follows:

Authority: 6 U.S.C. sec. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. sec. 301.

2. In appendix C to part 5, add paragraph 84 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

84. The DHS/CBP-018 Customs Trade Partnership Against Terrorism (CTPAT) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-018 CTPAT System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security activities. The DHS/CBP-018 CTPAT System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

No exemption shall be asserted with respect to information requested from and provided by the CTPAT Program applicant including, but not limited to, company profile, supply chain information, and other information provided during the application and validation process. CBP will not assert any exemptions for an individual's application data and final membership determination in response to an access request from that individual. However, the Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement agency has sought particular records may affect ongoing law enforcement activities. As such, pursuant to 5 U.S.C. sec. 552a(j)(2), DHS will claim exemption from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. sec.552a(k)(2), as is necessary and appropriate to protect this information.

Pursuant to exemption 5 U.S.C. sec.552a(j)(2) of the Privacy Act, all other CTPAT Program data, including information regarding the possible ineligibility of an applicant for CTPAT Program membership discovered during the vetting process and any resulting issue papers, is exempt from 5 U.S.C. secs. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. sec. 552a(k)(2), information regarding the possible ineligibility of an applicant for CTPAT Program membership discovered during the vetting process and any resulting issue papers are exempt from 5 U.S.C. secs. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). In addition, to the extent a record contains information from other exempt systems of records, CBP will rely on the exemptions claimed for those systems.

Finally, in its discretion, CBP may not assert any exemptions with regard to accessing or amending an individual's application data in the CTPAT Program or accessing their final membership determination in the CTPAT programs.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on

disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a

confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(j) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

James Holzer,
Acting Chief Privacy Officer,
U.S. Department of Homeland Security.

[FR Doc. 2021-05650 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]